MKM:TH/MKP
F. #2017R01840

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

Docket No. 18-204 (S-1) (NGG) (VNS)

- against -

KEITH RANIERE,
also known as "Vanguard,"
CLARE BRONFMAN,
ALLISON MACK,
KATHY RUSSELL,
LAUREN SALZMAN, and
NANCY SALZMAN,
also known as "Prefect,"

Defendants.

- X

MEMORANDUM OF LAW IN SUPPORT OF THE GOVERNMENT'S MOTION
TO PRODUCE FORENSIC COPIES OF ELECTRONIC DISCOVERY TO DEFENDANTS

RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

Moira Kim Penza
Tanya Hajjar
Assistant U.S. Attorneys
(Of Counsel)

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The government respectfully submits this memorandum of law in support of its motion to produce entire forensic copies of certain electronic evidence in its possession, pursuant to a protective order, to all defendants in the above-captioned case. The government seeks to provide forensic copies of this material in order to comply with its disclosure obligations and to expedite defendants' access to voluminous electronic materials containing material discoverable to defendants. For the reasons set forth below, the government's motion should be granted.

BACKGROUND

The defendants Keith Raniere, Clare Bronfman, Allison Mack, Kathy Russell, Lauren Salzman, and Nancy Salzman are charged by superseding indictment, returned July 23, 2018 with participating in a long-running racketeering conspiracy, among other crimes. These charges arise out of conduct related to several pyramid-structured organizations that Raniere founded in the Albany, New York area, including NXIVM and various related entities, as well as an organization referred to as "DOS," all of which offered purported self-help programs. As alleged in the superseding indictment, Raniere and an "inner circle" of individuals, including the defendants, comprised an organized criminal enterprise that engaged in various criminal activities with the aim of promoting Raniere and recruiting others into NXIVM and DOS for financial and personal benefits.

By this motion, the government seeks to disclose full forensic copies of certain devices in its possession to all defendants in the above-captioned case pursuant to the protective order entered by the Court on August 1, 2018. The devices consist of fifty-one

electronic devices, including external hard drives and thumb drives, belonging to defendant Nancy Salzman and seized from her residence (the "Oregon Trail Devices").[1]

I. Processing and Search of the Oregon Trail Devices

The Federal Bureau of Investigation ("FBI") provided the Oregon Trail Devices to its Computer Analysis and Response Team ("CART") to be imaged and processed at the commencement of its court-authorized search of those devices, which remains ongoing.

For each of the Oregon Trail Devices, CART examiners first undertook to image the device, that is, to make an exact copy of the data contained on the computer, with the use of specialized forensic imaging software that copies each bit of computer code—a series of ones and zeroes—in sequence, "bit by bit." To ensure that the original and the image are forensically identical, the CART examiner used a computer program to calculate a unique number, or "hash value" for the original and, later, for the image. The examiner then confirmed that the hash values for the originals matched the hash values for the forensic image, reflecting that the images were identical to the originals.

CART examiners then processed the data from each of the devices for review. From the bit-by-bit imaged copy, the CART examiner extracted all available data from the original hard drive media, including active data, deleted data, metadata, files, folders, and

---

[1] The Oregon Trail Devices consist of those electronic devices seized from Nancy Salzman's residence with the following designated item numbers: 1B111, 1B110, 1B108, 1B107, 1B106, 1B105, 1B104, 1B103, 1B102, 1B101, 1B99, 1B97, 1B96, 1B95, 1B94, 1B93, 1B92, 1B91, 1B90, 1B89, 1B88, 1B84, 1B83, 1B82, 1B81, 1B79, 1B78, 1B77, 1B76, 1B75, 1B73, 1B72, 1B70, 1B69, 1B68, 1B67, 1B66, 1B65, 1B64, 1B63, 1B62, 1B61, 1B60, 1B59, 1B58, 1B56, 1B55, 1B54, 1B52, 1B14, and 1B13. (See Gov't Letters Regarding Discovery, ECF Docket Nos. 141, 143 and accompanying lists.)

empty or unallocated space on the hard drive, making it available for further examination and review. On a rolling basis, the content of each device was then uploaded to an FBI data review platform, on which the FBI case agents began reviewing the data consistent with the court-authorized searches.

Initial searches of the Oregon Trail Devices have yielded significant amounts of material responsive to the search warrants authorizing their seizure, as well as audio, video, and other statements attributable to the defendants and other witnesses in this case.

II. Objections to Disclosure of the Oregon Trail Devices

On August 3, 2018, a little over a week after the defendants' arraignment on the superseding indictment on July 25, 2018, the government notified the defendants of the existence of the Oregon Trail Devices and requested that, to the extent any defendant objected to the disclosure of full discovery copies of such materials to all defendants, that it notify the government "as soon as possible and no later than August 8, 2018." Having received no objection, on August 28, 2018, the government notified defense counsel that discovery copies of certain of the Oregon Trail Devices were available to them for request from an outside vendor. Several hours later, the government received an email from counsel for Nancy Salzman objecting, for the first time, to the "distribution of items seized from our client—or places attributable to her—to anyone but us, unless such items are within the scope of the warrant and are established to not contain irrelevant, privileged, or otherwise confidential materials." Upon receipt of the email, the government halted production of any of these materials to any defendant other than Nancy Salzman.

III. Production of Electronic Discovery By A Vendor and Privilege Review

The government has retained a third-party vendor (the "Vendor") to assist in processing and producing electronic materials in its possession. The government has begun providing the Vendor with copies of materials from the FBI. Where feasible, the government will produce electronic materials to defendants in a form that can be loaded directly into a discovery management software system (such as Relativity or Concordance). However, some electronic materials, such as lengthy audio or video files, may not be able to be produced in this format.

Electronic data to which the government has been alerted to the existence of potentially privileged material, where feasible, will be uploaded to a separate "Firewall Database," which the government's trial team and the case agents (collectively, the "Trial Team") cannot access. Access to the Firewall Database is restricted to the government's Firewall Assistant United States Attorney. Of the Oregon Trail Devices, the government has been alerted by counsel for Nancy Salzman to the existence of potentially privileged material on eighteen devices belonging to Nancy Salzman (the "Potentially Privileged Material").[2]

[2] The Oregon Trail Devices with the following designated item numbers are those on which the government has been alerted to the existence of potentially privileged material: 1B103, 1B99, 1B95, 1B94, 1B88, 1B87, 1B84, 1B79, 1B75, 1B74, 1B73, 1B69, 1B61, 1B60, 1B57, 1B54, 1B52, and 1B14.

ARGUMENT

For the reasons set forth below, the government seeks to provide, to each of the defendants in this case, subject to a protective order, full forensic copies of the Oregon Trail Devices, except the Potentially Privileged Material.[3] Such disclosure is warranted because (1) based on initial searches conducted by the FBI, the Oregon Trail Devices contains large amounts of information discoverable to all defendants under Rule 16 as well as Title 18, United States Code, Section 3500; (2) the discoverable data is interspersed throughout the Oregon Trail Devices, making segregation of such data from non-responsive data within a single electronic storage medium impractical; (3) several defendants have not consented to the exclusion of speedy trial time and the government seeks to expedite their access to voluminous electronic discovery; and (4) a protective order will sufficiently address the privacy concerns of the defendant Nancy Salzman.

A preliminary review of the Oregon Trail Devices has indicated that a very large quantity of material on the Oregon Trail Devices consists of documents or files authored by other defendants or witnesses in this case, including NXIVM course materials and documents shared or authored by other defendants. See Fed. R. Crim. P. 16(a)(1)(A) (requiring the production of "any relevant written or recorded statements made by [a] defendant" within the government's possession).

---

[3] The government will first endeavor to segregate the Potentially Privileged Material from the non-potentially privileged material on the Oregon Trail Devices by running searches through the FBI's data review platform or through a discovery management software system. However, for certain devices and depending on the amount of Potentially Privileged Material, this may prove impractical. Should the Court grant the government's motion, the government will confer with counsel for Nancy Salzman to address these issues and, if appropriate, may seek additional guidance from the Court.

The government notes that provision of full forensic copies of electronic evidence, even to co-defendants, is common in this District, particularly in cases charging conspiracy or racketeering, where evidence of the relationships between alleged co-conspirators is necessarily relevant to the charges. See, e.g., United States v. Cooper, 17-CR-296 (PKC) (E.D.N.Y. 2018) (03/20/2018 Minute Entry) (finding no fault with government's provision of a Facebook account in full to co-defendants, over owner's privacy objection, where owner was accorded some limited time to identify and seek redactions of material).

I. Provision of Full Forensic Copies of the Oregon Trail Devices is Necessary For the Government To Satisfy Its Disclosure Obligations In This Case

The government submits that the nature of the potentially discoverable electronic data on the Oregon Trail Devices warrants provision of full forensic copies of the devices to defendants while the government's search of those devices is ongoing. The Second Circuit in United States v. Ganias, sitting en banc, addressed the difference between electronic evidence and hard copy evidence, as well as technical obstacles to segregating discoverable files within a single electronic storage medium:

> Though to a user a hard drive may seem like a file cabinet, a digital forensics expert reasonably perceives the hard drive simply as a coherent physical storage medium for digital data—data that is interspersed throughout the medium, which itself must be maintained and accessed with care, lest this data be altered or destroyed. Even the most conventional "files"—word documents and spreadsheets such as those the Government searched in this case—are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact "fragmented" on a storage device, potentially across physical locations. Because of the manner in which data is written to the hard drive, rarely will one file be stored intact in one place on a hard drive; so-called "files" are stored in multiple locations and in multiple forms. . . .

> "Files," in short, are not as discrete as they may appear to a user. Their interspersion throughout a digital storage medium, moreover, may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data. To be clear, we do not suggest that it is impossible to do so in any particular or in every case; we emphasize only that in assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular case—features that simply do not exist in the context of paper files.

United States v. Ganias, 824 F.3d 199, 212-13 (2d Cir.) (en banc) (internal quotation marks and citations omitted), cert. denied, 137 S. Ct. 569, 196 L. Ed. 2d 445 (2016). Consistent with these technological hurdles, courts have recognized that searches of electronic accounts may require a file-by-file review that should not be subject to strict time limits. See, e.g., United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) *26 ("[C]omputer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution."); United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) ("The Fourth Amendment only requires that the subsequent search of the computer be made within a reasonable time."), aff'd, 592 F.3d 826 (8th Cir. 2010); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) ("Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant."); see also United States v. Tairod Nathan Webster Pugh, No. 1:15-CR-00116-NGG, 2015 WL 9450598, at *27 (E.D.N.Y. Dec. 21, 2015) (collecting cases).

The Ganias court also explained that "nature of digital storage presents potential challenges to parties seeking to preserve digital evidence, authenticate it at trial, and establish its integrity for a fact-finder" and that "[p]reservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial." Id. at 215 (noting that the "extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium"). In United States v. Lumiere, the district court denied the defendant's motion to suppress electronic evidence that the government obtained from various digital storage devices, including a mobile phone, three computers, two tablets, seven USB flash drives, and two CD-ROM discs. No. 16-CR-483 (JSR), 2016 WL 7188149, at *2-4 (S.D.N.Y. Nov. 29, 2016). The court rejected the defendant's argument that the government violated the Fourth Amendment by failing to "segregate" evidence within the scope of the warrant from evidence outside the scope of the warrant. Citing Ganias, the Court distinguished paper files from digital files and explained that, with respect to hard drives containing electronic data, "meaningful digital segregation may well be impossible," justifying the government's retention of the full images of the devices. Id.; see also United States v. Manafort, 314 F. Supp. 3d 258, 271-72 (D.D.C. 2018) (upholding government's retention of images created during the execution of a search warrant given the need to authenticate exhibits at a later date).

Here, as in Ganias and Lumiere, material discoverable to the defendants under Rule 16 of the Federal Rules of Criminal Procedure and otherwise, is located in myriad files "interspersed throughout" the Oregon Trail Devices, Ganias, 824 F.3d at 212. Nearly all of the Oregon Trail Devices contain audio or video files of the defendant Keith Raniere or other

NXIVM content attributable to one or more of the defendants which is discoverable under Rule 16(a)(1)(A).

In addition, the government has identified files within the Oregon Trail Devices that may be "material to preparing [a] defense" within the meaning of Rule 16. As NXIVM's President, Nancy Salzman possessed years' worth of records relating to NXIVM and its affiliated entities. For example, some of the Oregon Trail Devices contain files which appear to contain confessions of "breaches" or other acknowledgements of purported personal failings authored by other defendants in the case. Not only is this enterprise evidence, but a defendant might seek to affirmatively use this information at trial or at sentencing to suggest reduced personal culpability.[4] Lastly, the government has also identified files within the Oregon Trail Devices attributable to witnesses in this case, bringing such files within the scope of the search and also discoverable to defendants pursuant to Title 18, United States Code, Section 3500 and, in some instances, Giglio v. United States, 405 U.S. 150 (1972).

This material may not be able to be fully digitally segregated from within the Oregon Trail Devices, and even if it could be segregated file-by-file (an extraordinarily time-consuming process), it would not "afford [the] defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the

---

[4] The government expresses no view as to the merits of such a potential defense argument. It merely notes the difficulty of identifying, at this early juncture, which files may assist defense counsel in "preparing [a] defense" within the meaning of Rule 16. By seeking disclosure of the full forensic copies of the Oregon Trail Devices to all defendants, the government seeks to expedite defendants' early access to such materials so that they may have adequate time to use them in preparing a defense.

authenticity or reliability of evidence allegedly retrieved . . . or to locate exculpatory evidence that the government missed." Ganias, 824 F.3d at 215. Based on its initial search, the Oregon Trail Devices contain evidence that would be admissible as to all defendants as enterprise evidence, among other things. Therefore, providing the full forensic copy solely to counsel for Nancy Salzman—as the government has already done—does not obviate the "interests of those [other] defendants in conducting their own forensic examination of the data in search of exculpatory evidence or to replicate and criticize the Government's inspection procedures." Id. at 216-17 & n.36; see, e.g., United States v. Kimoto, 588 F.3d 464, 480 (7th Cir. 2009) (evaluating defendant's motion to dismiss due to government's alleged failure to preserve and provide "complete forensic copy of all digital files" to the defendant); United States v. Burnett, No. 12-CR-2332-CVE, 2013 WL 12334143, at *4 (D.N.M. Mar. 8, 2013) (evaluating defense claim that government was obligated to provide defendant with "forensic copies of the hard drives of computers and electronic devices" seized from a third party).

Consistent with the search warrants obtained in this case, the government will continue to search non-privileged materials in its possession and produce the results of those searches to all defendants on a rolling basis. The interspersed material may draw its significant from its proximity to other material that provides attribution evidence, which is within the scope of the search. However, given that defendants have not uniformly consented to the exclusion of time for the purpose of plea negotiations, discovery production, and review and preparation for trial, the government seeks to expedite defendants' early access to the voluminous electronic material in its possession by providing, to all defendants, full forensic copies of the Oregon Trail Devices, except the Potentially Privileged Material.

II. Nancy Salzman's Privacy Concerns Can be Adequately Addressed By A Protective Order

The government notes that it has not yet identified any material within the Oregon Trail Devices that appears to raise an obvious privacy concern unrelated to the crimes charged in this case. The conspiracy charged in this case involves the intimate and near-daily association of the defendants for over a decade. Not surprisingly, therefore, the content of the Oregon Trail Devices includes data created by, or sent to, or related to, NXIVM and the defendants charged in this case. This case therefore "does not involve a more typical situation in which" law enforcement is searching "electronically-stored data associated with the alleged crimes on a hard drive that largely contains non-criminal information." United States v. Ulbricht, 858 F.3d 71, 103 (2d Cir. 2017), cert. denied, 138 S. Ct. 2708 (2018); cf. United States v. Wey, 256 F. Supp. 3d 355, 366 (S.D.N.Y. 2017) (noting significant privacy concern in search and seizure of all financial records, notes, records of internal and external communication without specifying crimes under investigation).

In any event, the defendants' privacy concerns can be adequately addressed by an appropriate protective order limiting disclosure of the Oregon Trail Devices. One district court, in weighing whether to provide a full copy of a third-party's hard drive to a defendant, concluded that production of the "entire copy" was appropriate and that a protective order would suffice to allay any privacy concerns regarding the third party's personal information. United States v. Savedoff, No. 16-CR-41G, 2017 WL 2305751, at *2–3 (W.D.N.Y. May 25, 2017) (observing that "personal information of third parties pervade[d] th[e] case" and noting the difficulty in determining "how much of this otherwise very personal information . . . somehow would be intertwined with other, more relevant information").

CONCLUSION

For the reasons set forth above, the government respectfully moves to produce, to all defendants in this case, full forensic copies of the Oregon Trail Devices, except the Potentially Privileged Material, pursuant to the protective order entered by the Court on August 1, 2018.

Dated: Brooklyn, New York
October 3, 2018

Respectfully submitted,

RICHARD P. DONOGHUE
UNITED STATES ATTORNEY
Eastern District of New York
271 Cadman Plaza East
Brooklyn, New York 11201

By: /s/ Tanya Hajjar
Moira Kim Penza
Tanya Hajjar
Assistant United States Attorneys
(718) 254-7000